EXPOSURE SECURITY

Executive Briefing: Atlassian to Use Customer Data

Published: April 17, 2026

See all Executive Briefings

Executive Summary

Background

Atlassian announced it will begin using customer metadata and in-app data from Jira, Confluence, and Jira Service Management (JSM) to improve its applications and AI experiences for all customers, effective **August 17, 2026**. This reverses Atlassian's previous public position, which explicitly stated that customer data wasn't used for AI model training. The announcement was made on April 16, 2026.

Atlassian is rolling out new organization-level settings in Atlassian Administration that let customers control their in-app data contribution. These settings are available gradually between now and May 19, 2026. However, the degree of control depends on your subscription tier, and certain data categories (metadata) can't be opted out of on most plans.

To check your current plan tier, go to **Atlassian Administration → Billing**. Your plan tier determines your default data contribution settings and the level of control you have over them (see *Default Settings by Plan Tier* in the Full Analysis).

Who It Applies To

This change affects all Atlassian Cloud customers on any active plan, including trials. It initially covers data in Jira, Confluence, JSM, and their associated Platform apps (Rovo, Home, Teams, Projects, Assets, Goals, Analytics, and Administration). Atlassian said it will notify customers when settings become available for additional apps.

If you manage multiple Atlassian cloud organizations, each one must be configured separately. Each organization has its own data contribution settings, determined by its own highest active plan tier.

What Does it Mean to Me?

Free and Standard plans: default opt-in. Organizations on Free or Standard plans will have in-app data contribution turned **on** by default. Atlassian will begin using the content of your Jira issues, Confluence pages, and JSM tickets to improve its products unless you actively disable this setting before August 17.

Premium and Enterprise plans default to off for in-app data. Organizations on Premium or Enterprise plans will have in-app data contribution turned **off** by default. However, Premium customers can't opt out of metadata contribution. Only Enterprise customers can disable metadata contribution entirely.

Metadata is always contributed on Free, Standard, and Premium plans. Regardless of your in-app data settings, metadata is always contributed on these plans. This setting can't be changed. Organizations for which metadata contribution is a concern have one option: upgrade to Enterprise, which carries significant cost implications that should be weighed against the risk.

Trial plans count toward your defaults. Your defaults are set by the highest active plan in your organization, including active trials. If a Premium or Enterprise trial expires, your organization may revert to Free/Standard defaults, which would silently re-enable in-app data contribution. Monitor plan expirations accordingly.

Vendor risk assessment. Reversing a stated policy position is itself a risk signal. Organizations maintaining vendor risk registers should update Atlassian's entry to reflect this change, particularly if data handling commitments were documented as part of the initial vendor assessment.

Key Dates

- **Now through May 19, 2026:** New data contribution settings rolling out gradually in Atlassian Administration
- **May 19, 2026:** Atlassian will send a reminder email; all settings should be available by this date
- **August 17, 2026:** Atlassian begins using data according to your contribution settings; updated legal terms take effect

How to Respond

1. **Identify your plan tier and check settings** *(Atlassian Admin)*. Go to Atlassian Administration → Billing to confirm your plan tier, then check Security → Data Contribution for the new settings. If the Data Contribution page isn't visible yet, keep checking; the settings are rolling out gradually.
2. **Disable in-app data contribution** *(Atlassian Admin)*. Once the settings appear, set in-app data contribution to **Off** for your organization. If you're on a Free or Standard plan, this is especially urgent because the default is On.

3. **Exclude specific spaces and apps** *(Atlassian Admin)*. Even if you choose to leave in-app data contribution on, exclude any Confluence spaces, Jira projects, or Teamwork Graph connectors that contain sensitive, regulated, or third-party data.
4. **Review updated legal terms** *(Legal)*. Have legal review the updated legal terms Atlassian referenced and flag anything that suggests certain data categories remain in scope even after opt-out.
5. **Assess compliance impact** *(Security / Compliance)*. Organizations with compliance obligations (HIPAA, SOC 2, GDPR, PCI DSS, CMMC, etc.) should assess whether contributing any data to Atlassian's improvement pipeline conflicts with their compliance posture or existing data processing agreements.
6. **Update vendor risk register** *(Security)*. Update Atlassian's entry in your vendor risk register to reflect this change. If data handling commitments were part of the original vendor assessment, note the reversal.
7. **Brief stakeholders** *(CISO / CIO)*. Inform executive leadership about this change and the actions taken. Organizations where SaaS data governance is a Board-level concern should prepare a summary for the audit committee or Board.
8. **Confirm opt-out before August 17** *(Atlassian Admin)*. Set a shared calendar reminder for early August to verify that your data contribution settings reflect your organization's intent. If you miss the deadline, your data begins flowing to Atlassian's improvement pipeline according to your plan's defaults.

Full Analysis & Recommendations follows

Full Analysis and Recommendations

Context: A Shift in Position

Until this announcement, Atlassian maintained a clear public position: customer data wasn't used to train, fine-tune, or improve AI models. Their AI Trust page and support documentation explicitly stated this for both Atlassian's own models and third-party providers (such as OpenAI) used by features like Rovo and Atlassian Intelligence. Their CTO reiterated this position publicly as recently as late 2025. The new data contribution model reverses that stance.

This change is separate from Atlassian Intelligence itself. Atlassian Intelligence (Rovo, AI-powered search, etc.) processes data on a per-request basis and, according to Atlassian, still doesn't retain or train on those inputs/outputs. The new data contribution model instead covers a broader, ongoing use of your metadata and in-app content to improve Atlassian's applications and AI experiences across all customers.

The practical question organizations should be asking: could Atlassian's use of contributed data result in patterns, structures, or insights from one customer's data surfacing in features or suggestions visible to other customers? Atlassian says it applies aggregation and de-identification, but hasn't published the specific techniques used, and these safeguards haven't been independently audited.

Default Settings by Plan Tier

Your default data contribution settings are determined by the highest active plan in your Atlassian organization, including trials:

- **Free / Standard:** Metadata is always contributed (can't disable). In-app data contribution defaults to **On**. You can opt out of in-app data only.
- **Premium:** Metadata is always contributed (can't disable). In-app data contribution defaults to Off. You can opt out of in-app data only.
- **Enterprise:** Metadata contribution defaults to On but can be disabled. In-app data contribution defaults to Off. You can opt out of **both metadata and in-app data**.

Metadata vs. In-App Data

Metadata is described by Atlassian as usage telemetry and structural information about how your organization uses Atlassian products. Atlassian hasn't published a precise list of what this includes. It likely covers project names, workflow configurations, issue type distributions, user counts, feature usage patterns, and similar structural data. On Free, Standard, and Premium plans, this category can't be opted out of.

In-app data includes the actual content of your Jira issues, Confluence pages, JSM tickets, and connected data from Teamwork Graph connectors. This is the category you can control via the new settings.

Important: If your organization has connected third-party data sources via Teamwork Graph (Google Drive, Slack, SharePoint, etc.), the in-app data contribution setting may extend to content pulled from those external systems. This significantly expands the scope beyond Jira and Confluence content alone. Review and exclude individual Teamwork Graph connectors as needed.

Trial Plan Reversion Risk

Your defaults are set by the *highest active plan* in your organization, including trials. If your organization is on a Standard plan and activates a Premium trial, in-app data contribution defaults to Off for the trial's duration. When that trial expires, the organization reverts to Standard-tier defaults, and in-app data contribution silently re-enables to On. Atlassian says it will notify you and give you 30 days to review settings after a downgrade, but this requires active monitoring.

Data Residency and Compliance Considerations

Organizations that configured data residency in Atlassian (restricting data to specific geographic regions) should determine whether contributed data stays subject to those residency constraints or gets processed elsewhere for AI improvement. This is particularly relevant for GDPR compliance and cross-border data transfer obligations. Atlassian's documentation doesn't currently address this interaction.

Organizations using Atlassian Guard data security policies (to restrict exports, block Marketplace app access, prevent public links, etc.) should determine whether those controls affect data contribution. Based on current documentation, data contribution settings appear to operate independently of Guard policies.

If your Atlassian instance contains data from clients, partners, or other third parties, contributing that data to Atlassian's improvement pipeline may conflict with your contractual obligations or data processing agreements. This applies to both in-app data and metadata: even structural information like project names or workflow configurations could reveal client-specific details.

Verification and Monitoring

Atlassian hasn't published clear guidance on how to verify that the opt-out took effect beyond checking the toggle in Atlassian Administration. Organizations should:

- Check Atlassian's audit log for events related to data contribution setting changes. Navigate to Atlassian Administration → Security → Audit log and filter for relevant events.
- Set up monitoring or alerts (if available) to detect if someone, or a plan change, re-enables data contribution after it's been disabled.

- Screenshot the Data Contribution settings page as evidence of your organization's opt-out status for compliance records.

New App and New Space Behavior

When you add a new app to your organization, Atlassian applies a **30-day delay** before data from that app is contributed. This gives you time to review and adjust settings. However, when you add a new Confluence space to an existing app, data contribution begins immediately according to your current settings. IT Admins should communicate this distinction to teams creating new spaces and confirm that organization-level defaults reflect the desired posture.

Recommended Actions

Immediate (Before May 19, 2026)

1. Monitor Atlassian Administration for the new Data Contribution settings to appear under Security → Data Contribution. *(Atlassian Admin)*
2. Once available, disable in-app data contribution across Jira, Confluence, and JSM. *(Atlassian Admin)*
3. Document your current organization ID(s) and plan tier(s). If you manage multiple organizations, repeat for each. *(Atlassian Admin)*
4. Forward the notification email from Atlassian to your security and legal teams. *(Atlassian Admin / CISO)*
5. Have legal review the updated legal terms Atlassian referenced and flag anything that suggests certain data categories remain in scope even after opt-out. *(Legal)*

Before August 17, 2026

1. Confirm the opt-out is in place and covers all relevant apps, spaces, and Teamwork Graph connectors. Screenshot the settings page for compliance records. *(Atlassian Admin)*
2. Verify whether data residency settings apply to contributed data, or whether contributed data is processed outside your configured region. *(Security / Legal)*
3. If your organization is on a Free or Standard plan and metadata contribution is a concern, evaluate whether upgrading to Enterprise is justified for the additional data governance controls. *(CIO / Finance)*
4. Assess whether any connected Teamwork Graph data sources (Google Drive, Slack, etc.) require exclusion from data contribution. *(Security / Atlassian Admin)*
5. Update Atlassian's entry in your vendor risk register. *(Security)*
6. Set a calendar reminder for early August to verify settings before the August 17 effective date. *(Atlassian Admin)*

Ongoing

- When adding new apps or Confluence spaces, verify that your organization-level data contribution settings apply correctly. New apps have a 30-day grace period before data is contributed; new spaces within existing apps do not. *(Atlassian Admin)*
- Monitor plan expirations, especially trials. A trial expiring can revert your defaults and silently re-enable in-app data contribution. *(Atlassian Admin)*
- Monitor Atlassian's communications for when data contribution settings become available for additional apps beyond Jira, Confluence, and JSM. *(Atlassian Admin / CISO)*
- If your plan tier changes (upgrade or downgrade), review your data contribution settings. Downgrading from Enterprise removes the ability to control metadata contribution. *(Atlassian Admin / CIO)*
- Check the audit log periodically for any changes to data contribution settings, whether from personnel or from plan-tier changes. *(Security / Atlassian Admin)*